# Eurocrypt 2012 Rump Session

#### Thanks to:

Sasha Boldyreva, Irina Warinschi and Bristol Crypto Group



Sponsored by Good Technologies

(Example only)

Which famous football player was spotted dancing by an overly excited Phong in the evening hours of Eurocrypt once.

(Example only)

Which famous football player was spotted dancing by an overly excited Phong in the evening hours of Eurocrypt once.

Ronaldinho

Which cryptographer completes the pair? Bellare—???

Which cryptographer completes the pair? Bellare—???

Rogaway



Who's the lookalike cryptographer?



Who's the lookalike cryptographer?

David Pointcheval

What is the url of the Bristolian crypto blog?

What is the url of the Bristolian crypto blog?

http://bristolcrypto.blogspot.co.uk

What was advertised endlessly during last year's Eurocrypt rump?

What was advertised endlessly during last year's Eurocrypt rump?

open postdoc positions at Bristol



What is the name of the "crypto-character" in this movie?



What is the name of the "crypto-character" in this movie?

Bogdan (the dodgy guy sprung from prison)

MI:4 Ghost Protocol

Which cryptographer completes the pair? ???-Shoup

Which cryptographer completes the pair? ???-Shoup

Cramer

How were people encouraged to keep the time at AC'01 rump?

How were people encouraged to keep the time at AC'01 rump?

They received candies if they finished on time

What do these conferences have in common? PKC'02, CHES'02, Euro'04, FSE'10, PKC'10

What do these conferences have in common? PKC'02, CHES'02, Euro'04, FSE'10, PKC'10

all had 2 Program co-Chairs

Which cryptographer completes the pair? Diffie—???

Which cryptographer completes the pair? Diffie—???

Hellman

What do these people have in common? Moti Yung, David Naccache, Gregor Leander, David Wagner

What do these people have in common? Moti Yung, David Naccache, Gregor Leander, David Wagner

Published at all 7 different IACR venues

Which Eurocrypt general chair performed in a band as part of the social program?

Which Eurocrypt general chair performed in a band as part of the social program?

Ivan Damgård

Which famous band played a free concert on the free afternoon of Eurocrypt once?

Which famous band played a free concert on the free afternoon of Eurocrypt once?

Queen

Which Champions League final took place during a past Eurocrypt?

Which Champions League final took place during a past Eurocrypt?

Milan-Liverpool



What is the name of the "crypto-character" in this movie?



What is the name of the "crypto-character" in this movie?

Miranda Frost James Bond, Die Another Day

Who is often referred to as the Dancing Cryptographer?

What do these people have in common? Eike Kiltz, Eike Kiltz, Eike Kiltz, Vanessa Vitse

What do these people have in common? Eike Kiltz, Eike Kiltz, Eike Kiltz, Vanessa Vitse

Won a Eurocrypt BPA

Which former IACR secretaries still regularly receive spam email on secretary@iacr.org?

Which former IACR secretaries still regularly receive spam email on secretary@iacr.org?

Benaloh, Black, Shrimpton



Who's the lookalike cryptographer?



Who's the lookalike cryptographer?

Tom Shrimpton

Who has served most years on the IACR Board?

Who has served most years on the IACR Board?

Tom Berson



Who's the lookalike cryptographer?



Who's the lookalike cryptographer?

Michel Abdalla

"Again, with many thanks for your pleasant Christmas surprise, and wishing you a happy Christmas and a good 1982,"

What was the surprise?



extensive, so I assume that you are not interested in co-authoring my paper and including the algorithm there. I would obviously be interested in that . If you now also improve the main algorithm it becomes entirely your paper! In any case, I hope you keep me informed it you publication plans, since I would at least like to mention what you did. - Do you know whether the proble. to find the shortest non- sero vector in a lattue is NP hand? It is for the max |x: |- now, but Peter can, to his instation, not extend the most to the Enclider case. My "prime number factory" is just starting, and the preliminary results are encouraging: mutter of & go depits in < 1 minute, and still meny improvements (making it 2 or 3 times as (ast) possible. again, with many thanks for and wishing you a happy Christness Hendrik Leustra and a good 1482.

"Again, with many thanks for your pleasant Christmas surprise, and wishing you a happy Christmas and a good 1982,"

What was the surprise?

Lovasz's letter containing an explanation of the basic reduction algorithm at the core of LLL.



What was the most uttered noun during the most recent Crypto rump?

What was the most uttered noun during the most recent Crypto rump?

leakage

Where was the first vegetation-based computer allegedly built?

Where was the first vegetation-based computer allegedly built?

David Naccache's sister's bathroom

Which Russian gift prompted a rump talk?

Which Russian gift prompted a rump talk?

Spinning glass globe

How many degrees was it at CHES held at EPFL?



How many degrees was it at CHES held at EPFL?

3 (Angle)



What is the name of the "crypto-character" in this movie?



What is the name of the "crypto-character" in this movie?

John Nash A Beautiful Mind

Whose sabattical enabled the advent of public key cryptography?

Whose sabattical enabled the advent of public key cryptography?

John McCarthy



What is the name of the "crypto-character" in this movie?



What is the name of the "crypto-character" in this movie?

Julius Caesar Cleopatra



What is the name of the "crypto-character" in this movie?



What is the name of the "crypto-character" in this movie?

James Douglas Clayton  $The\ Recruit$ 

What can be gruesome about extremal pruning?

What can be gruesome about extremal pruning?

Hacking off of limbs

What do these conferences have in common? Eurocrypt'02, Crypto'02, Eurocrypt'06, FSE'09

What do these conferences have in common? Eurocrypt'02, Crypto'02, Eurocrypt'06, FSE'09

Palindromic LNCS volume numbers



Who's the lookalike cryptographer?



Who's the lookalike cryptographer?

Krzysztof Pietrzak